A REVIEW OF SECURITY ALGORITHMS IN CLOUD COMPUTING ENVIRONMENT

P.Pushpa[1], Dr. G.N.K.Suresh Babu[2]
[1]Research Scholar, Department of Computer Applications, Bharathiyar University, Coimbatore
[2]Associate Professor, Acharya Institute of Technology, Bangalore.

ABSTRACT
Cloud Computing is an emerging technology today. Everyone in industries and academics they are moving data to cloud computing. Here the main question arises is, how far the cloud computing environment will provide data security? The main aim of this paper is to deal with different types of security algorithms and how we can keep the data safe. We can start with cloud computing types, deployment models and other basic information about the cloud computing and then we can move to the review of security algorithms and finally we can find out that which security algorithm gives more security to the data.
Keywords: Cloud Computing, public, private, hybrid, IAAS, SAAS, PAAS.

1 INTRODUCTION

Cloud Computing has become one of the most interesting technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering. The market research and analysis firm IDC suggests that the market for Cloud Computing services was $80billion in 2020 and will rise to $125billion/year by 2025. It has been estimated that the cost advantages of Cloud Computing to be three to five times for business applications and more than five times for consumer applications. Cloud Computing is a term used to describe both a platform and type of application. As a platform it supplies, configures and reconfigures servers, while the servers can be physical machines or virtual machines. On the other hand, Cloud Computing describes applications that are extended to be accessible through the internet and for this purpose large data centers and powerful servers are used to host the web applications and web services.

2 TYPES OF CLOUD COMPUTING

Cloud computing employs a service-driven business model. In other words, hardware and platform-level resources are provided as services on an on-demand basis. Conceptually, clouds offer services that can be grouped into three categories: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

1. Infrastructure as a Service: IaaS provide on-demand provisioning of infrastructural resources and does not manage or control the infrastructure and only manage and control the storage, application and selected network components. The cloud owner who offers IaaS is called an IaaS provider. Examples: Amazon EC2 .
2. Platform as a Service: PaaS providing software development frameworks and platform layer resources including operating system support. In PaaS user controls their application and does not manage servers and storage. Examples: Google App Engine, Microsoft Windows Azure etc.
3. Software as a Service: SaaS providing on demand applications all over the Internet. In SaaS user does not control or manage the servers, storage, network and application. Examples: Rack space etc.

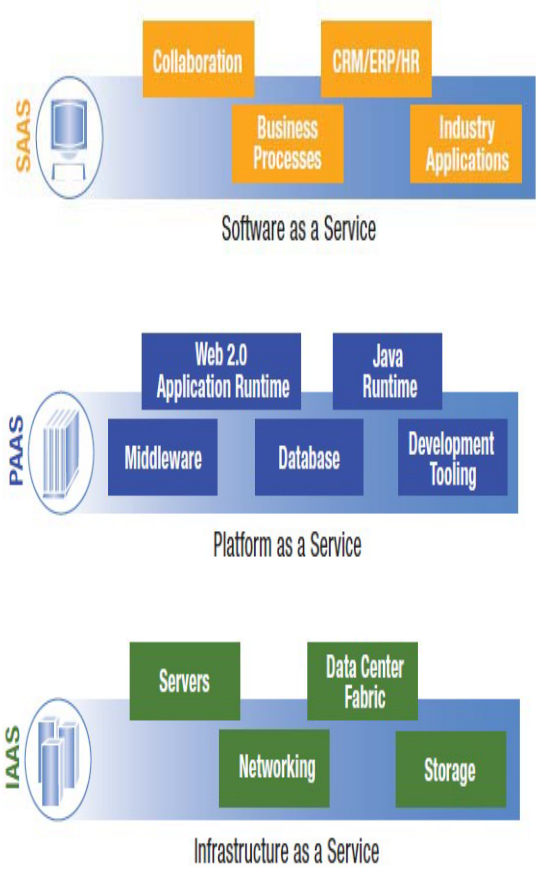

Fig.1 Represents SaaS, PaaS, IaaS

Fig.1 represents how cloud computing can be linked with other services.

3 DEPLOYMENT MODELS

1. Public Clouds are publicly accessible and in this types of clouds are managed by third party.
2. Private Clouds are only accessible in private network. Private cloud infrastructure made available only a specific member and managed by organization itself or third party service provider.
3. Community Clouds are only accessible to a few numbers of clients with known features.
4. Hybrid Clouds are composition of two or more clouds. The cloud service providers submit to a number of advantages cloud computing offers: from nominal costs because of the short of investment in, for example, hardware, to higher and quicker adaptability to the requirements of the client, and the suspected lower costs of repairs, support and other services attached to the ICT human resources. In some models, often all you require is access to the internet, a web browser.

4 LITERATURE SURVEY

Jing-Jang Hwang et al. [1], has proposed a business model for cloud computing for data security using data encryption and decryption algorithms. In this method cloud service provider has responsible for data storage and data encryption/decryption tasks, which takes more computational overhead for process of data in cloud server. The main disadvantage of this method is, there is no control of data for data owner i. e, data owner has completely trusted with cloud service provider and he has more computational overhead.

Junzuo et al. [2], proposed an Attribute Based Encryption (ABE) and verifiable data decryption method to provide data security in cloud based system. They have been designed the data decryption algorithm based on the user requested attributes of the out sourced encrypted data. One of the main efficiency drawbacks of this method is, cloud service provider has more computational and storage overhead for verification of user attributes with the outsourced encrypted data. While introducing third party auditor we can reduces the storage, computation, and communication overheads of the cloud server, which improves the efficiency of the cloud data storage.

FatemiMoghaddam et al. in [3], discussed the performance of six different symmetric key RSA data encryption algorithms in cloud computing environment. They have proposed two separate cloud servers; one for data server and other for key cloud server and the data encryption and decryption process at the client side. The main drawback of this method is to maintaining two separate servers for data security in cloud, which creates a more storage and computation overheads.

Brian Hay et. al [4] have focused on data authentication, data integrity, querying and outsourcing the encrypted data. Their research says that, the risks can arise at operational trust modes, resource sharing, new attack strategies. In operational trust modes, the encrypted communication channels are used for cloud storage and do the computation on encrypted data which is called as homomorphic encryption[5]. New attack strategies like Virtual Machine Introspection (VMI) can be used at virtualization layer to process and alter the data.

Kevin Curran et.al [6] mentions that Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud computing has become a variable platform for companies to build their infrastructures upon. If companies are to consider taking advantage of cloud based systems by storing their data in Cloud Storage they will be faced with the task of seriously reassessing their current security strategy.

Randeep Kaur et.al [7] mentions some of the notable challenges associated with cloud Storage. The challenges are Security, Privacy and Lack of Standards which slow down services in the cloud.

Rashmi Nigoti et.al [8] defines some privacy and security-related issues that are believed to have long-term significance for cloud storage.

5 EXISTING SECURITY ALGORITHMS

5.1 Data Encryption Standard Algorithm

DES is very commonly used symmetric key algorithm. It was developed by IBM in 1974, but now a days many methods are found that had proven this algorithm unsecured. In DES algorithms block cipher is of 64 bits and key used is of 56 bits out of 64 bits of key is used rest of 8 bits are padded. In block cipher we encrypt block of data which consist of plain text by combination of confusion and diffusion to make cipher block then this cipher block has to pass 16 rounds, before passing through these 16 rounds the 64 bits of data is divided into 32 bits. After dividing the data into 32 bits, F-function (Feistel function) is applied. F-function consists of substitution, permutation, key mixing. The output of function is combined with other half of the data using XOR gate alternate crossing of data is done; then crossing of data is done. After doing 16 such rounds cipher text is produced or encryption of data is done. To decrypt the data reverse operation is done. The drawback of DES is that key used in DES is very small and its security can be broken easily and DES works fast on hardware only and woks slowly on software. Data bits are divided into two parts Lf and Rf than F function and XOR operation is applied on Rf, and output is combined with Lf.

5.2 Advance Encryption Algorithm (AES)

Advance Encryption algorithm AES is also known as Rijndael. AES is announced as U.S FIPS by NIST in 2001. In AES, different size of key is used i.e. 128, 192 or 256 bits, depends on how many cycle it uses. For 10 cycles 128-bit key, 12 cycles 192 bit key and for 14 cycles 256 bit key is used. All rounds of AES are similar except the last one. AES works on 4x4 matrixes. AES consists of key expansion, initial and final round. Initial round consist of Add Round Key, Sub Bytes, Shift Rows, Mix Columns, Add Round Key and final round also consists of similar function as initial round except mix columns. AES works fast on both software and hardware.

5.3 Triple- DES (TDES)

TDES is enhanced version of DES in TDES the key size is increased to increase i.e. 168 bits the security of data. In TDES only size of key is increased rest of the working is similar to DES. In TDES three different keys are applied on cipher block.

5.4 Blowfish Algorithm

Blowfish Algorithm is a symmetric key algorithm which was developed in 1993 by Bruce Schneier. Its working is almost similar to DES but in DES key size is small and can be decrypted easily but in Blowfish algorithm the size of key is large and it can vary from 32 to 448 bits. Blowfish also consists of 16 rounds like DES . Blowfish algorithm can encrypt data having size multiple of eight and if the size of the message is not multiple of eight than bits are padded. In Blowfish algorithm also 64 bits of plain text is divided into two parts of size 32 bits. One part taken as the left part of message and other is right part of message. The left part is XOR with the elements of P-array which creates some value, then that value is passed through transformation function F. The value originated from the transformation function is again XOR with the other half of the message i.e. with right bits, then F| function is called which replace the left half of the message and P| replace the right side message.

5.5 Homomorphic Encryption

Homomorphic encryption uses asymmetric key algorithm in which two different keys are used for encryption and decryption i.e. public key and private key. In mathematics homomorphic

means conversion of one data set to another, without losing its relation between them. In homomorpic complex mathematics functions are applied to encrypt the data and similar but reverse operation is applied to decrypt the data.

5.6 RSA

RSA was invented by Ranold Fivest, Adi Shamir and Leonard Adleman in 1977. RSA is also an asymmetric algorithm. Functioning of RSA is based on multiplication of two large numbers. Two large prime numbers are generated and multiplied. After multiplying two numbers, modulus is calculated the number that is generated is used as the public and private key. The two numbers that are used for multiplication-one of them is public other is private. Steps for RSA algorithm:-

a) Divide the large message into small number of blocks where each block represents the same range.

b) By raising the eth power to module n encrypt the message.

c) For the decryption of message increase another power d module n.

5.7 Diffie- Hellman Key Exchange

Diffie Hellman key exchange algorithm was developed by Whitfield Diffie and Martin Hellman in 1976. Diffie Hellman also required two different keys. In Diffie Hellman Key Exchange, a shared secret key established, that is used that is used for communication over the public network. In Diffie Hellman Key Exchange Algorithm Sender and Receiver picks two secret numbers and these numbers are known to both sender and receiver. Let the number selected by sender is Ns and number selected by receiver is Nr then sender and receiver will generate a secrete key by calculating Ta.

Ts= gsr mod p

Here, g =|p|

p is a large prime number

g < p

After calculating Ts and Tr, sender and receiver will exchange their values with each other, if they find that both the values are same, then communication starts.

5.8 RC5

It was developed in 1994. The key length if RC5 is MAX2040 bit with a block size of 32, 64 or 128. The use of this algorithm shows that it is Secure. The speed of this algorithm is slow.

5.9 EI Gamel

In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It was described by Taher Elgamal in 1984. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption. ElGamal encryption can be defined over any cyclic group G . Its security depends upon the difficulty of a certain problem in G related to computing discrete logarithms.

5.10 *IDEA*

International Data Encryption Algorithm was proposed by James Massey and Xuejia Lai in 1991.It is considered as best symmetric key algorithm. It accepts 64 bits plain text and key size is 128 bits. IDEA consists of 8.5 rounds. All rounds are similar except the one. In IDEA the 64 bits of data is divided into 4 blocks each having size 16 bits. Now basic operations modular, addition, multiplication, and bitwise exclusive OR (XOR) are applied on sub blocks. There are eight and half rounds in IDEA each round consist of different sub keys. Total number of keys used for performing different rounds is 52. In round 1 the K1 to K6 sub keys are generated, the sub key K1 has the first 16 bits of the original key and K2 has the next 16 bits similarly for K3, K4, K5 and K6. Therefore for round 1 (16*6=96) 96 bits of original cipher key is used.

6 CRYPTOGRAPHY

Cryptography can help emergent acceptance of Cloud Computing by more security concerned companies. The first level of security where cryptography can help Cloud computing is secure storage. Cryptography is the art or science of keeping messages secure by converting the data into non readable forms. Now a day's cryptography is considered as a combination of three algorithms. These algorithms are Symmetric-key algorithms, Asymmetric-key algorithms, and Hashing. In

Cloud computing, the main problems are related to data security, backups, network traffic, file system, and security of host, and cryptography can resolve these issues to some extents. Consider an example, In the cloud consumer can protect its confidential data, then he has to encrypt his information before storing in the cloud storage, and it is advised not to save an encryption key on the same server where you have stored your encrypted data. This will helps us in reduction of Virtualization vulnerability. For secure communication between the host domain and the guest domain, or from hosts to management systems, encryption technologies, such as Secure HTTP (HTTPS), encrypted Virtual Private Networks (VPNs), Transport Layer Security (TLS), Secure Shell (SSH), and so on should be used. Encryption will help prevent such exploits as man-in-the-middle (MITM), spoofed attacks, and session hijacking.

7 DATA SECURITY IN CLOUD COMPUTING

Major concern is security of data. Data relocation on high level has negative implications for data safety and data security as well as data availability. Thus the main apprehension with reference to safety of data residing in the Cloud is: at the rest how to safe security .Although, customers know the location of data and there in no data mobility, there are question relating to its security and secrecy of it. No confusion the Cloud Computing area has become bigger because of its wide network access and exibility. But we can also rely in terms of a safe and secure atmosphere for the personal data and info of the user is being required.

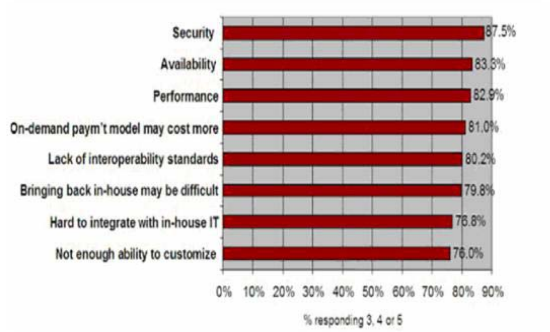

Fig 2: Ranking of security in cloud computing as surveyed by IDC.

Fig: 2 shows the survey on security. This represents security as first rank according to IT executives. This information is collected from 263 IT professional by asking different question related to the cloud, and many of the executives are worried about security perspective of cloud. [12]

8 CLOUD COMPUTING SECURITY CONCERNS

Two main issues exist with security and privacy aspects of Cloud Computing: 1. loss of control over data and 2.dependence on the Cloud Computing provider. These two issues can lead to a number of legal and security concerns related to infrastructure, identity management, access control, risk management, regulatory and legislative compliance, auditing and logging, integrity control as well as Cloud Computing provider dependent risks.

Typical issues due to the loss of control over data are:

1. Most customers are aware of the danger of letting data control out of their hands and storing data with an outside Cloud Computing provider. Data could be compromised by the Cloud Computing provider itself or other competitive enterprises which are customers with the same Cloud Computing provider. There is a lack of transparency for customers on how, when, why and where their data is processed. This is in opposition to the data protection requirement that customers know what happens with their data.

2. Many Cloud Computing providers are technically able to perform data mining techniques to analyse user data. This is a very sensitive function and even more so, as users are often storing and processing sensitive data when using Cloud Computing services. This holds especially true for social media applications that encourage users to share much of their private life e.g. private photos.

3. Mobile devices, in particular with their limited storage and computing capabilities are drivers for having services provided by Cloud Computing instead of using software on individual computers. Even data that are only to be transferred from one mobile device to another (local) device, are often transferred via the cloud, when cloud oriented applications on the mobile devices are involved. Therefore

users often put themselves at risk without noticing this, as they assume that the data is transferred locally.

4. Since Cloud Computing is a service, it has to be accessed remotely. The connection between the Cloud Computing provider and customer is not always adequately protected. Security risks that threaten the transfer line include eavesdropping, DNS spoofing, and Denial-of-Service attacks.

5. Concerns also exist with regard to deletion of data: It is difficult to delete all copies of electronic material because it is difficult to find all copies. It is impossible to guarantee complete deletion of all copies of data. Therefore it is difficult to enforce mandatory deletion of data. However, mandatory deletion of data should be included into any forthcoming regulation of Cloud Computing services, but still it should not be relied on too much: the age of a "Guaranteed complete deletion of data", if it ever existed has passed. This needs to be considered, when data are gathered and stored.

6. Data Protection and Privacy legislation is not even similar in many countries around the globe yet Cloud Computing is a global service of the future. Consequently the problems and risks that affect data protection rules in Europe must be considered properly when Cloud Computing platforms are located on servers in non-European countries.

7. Cloud computing depends on a reliable and secure telecommunications network that assures and guarantees the operations of the terminal users of the services provided in the cloud by the cloud computing provider. Telecommunications networks are often provided separately from the Cloud computing services.

Typical issues with regard to the dependence on the Cloud Computing provider are:

1. A major concern regarding dependence on a specific Cloud Computing provider is availability. If the Cloud Computing provider were to go bankrupt and stopped providing services, the customer could experience problems in accessing data and therefore potentially in business continuity.

2. Some widely used Cloud Computing services (e.g. GoogleDocs) do not include any contract between the customer and Cloud Computing provider. Therefore a customer does not have anything to refer to if incidents occur or any problems arise.

3. Cloud Computing is a service similar to other more "traditional" services and utilities (e.g. telecommunication, transaction banking, electricity, gas, water, etc.) Both Cloud Computing services and traditional services and utilities tend to be offered by large providers dealing with smaller customers. Therefore the customers usually depend on the providers because it is difficult to change providers if it is possible at all. Consequently traditional services (e.g. telecommunication, transaction banking, electricity, gas, water, etc.) are usually regulated with regard to the functionality range (e.g. mandatory functions, coverage), pricing, liability of the provider, and reliability. Cloud Computing colloborates a trend that ICT security is no longer a purely technical issue but an issue between individuals and organisations and thus includes both human and organisational aspects such as management, contracting, and legal enforcement.

9 OBJECTIVE OF OUR PROPOSED SYSTEM

1. To develop a system that will Provide Security and Privacy to Cloud Storage
2. To Establish an Encryption Based System for protecting Sensitive data on the cloud and Structure how owner and storage Service Provider to operate on encrypted Data
3. To Create a System where the user store its data on the cloud the data is sent and stored on the cloud in encrypted form As in normal cases in cloud computing when a user login to the cloud and they store data on cloud storage device the data stored on the server cloud is not much secure as it can be readable to anyone which have permission to access and Leaving data vulnerable,
4. To Develop a retrieval System in which the data is retrieved by the user in encrypted form and is decrypted by the user at its own site using a public and private key encryption both the keys working at the user level.

10 PROPOSED PLAN

Our main intention is, how we can provide data security in cloud computing. We are trying to give better solution than the existing one. To access a cloud based web application that will try to eliminate the concerns regarding data privacy, segregation. We proposed different encryption algorithms like - AES, DES, RSA and Blowfish to ensure the security of data in cloud. For the perspective of different users, we proposed these algorithms. DES is developed in early 1970s; Blowfish is developed by Bruce Schneier, in 1993. AES is developed by NIST in 2001.All of these algorithms are symmetric key, in which a single key is used for encryption/decryption purposes. RSA is asymmetric key algorithm, created by Ron Rivest, Adi Shamir and Lenard Adleman in 1978. This algorithm is used for public key cryptography. In this, two public/private keys are used for encryption/decryption. The key-size of algorithms is different. Like-Key size of Blowfish algorithm is 128-448 bits and AES algorithm is 128,192,256 bits. The key length of AES is less than Blowfish. 2048 bits of asymmetric key is equivalent to 112 bits of symmetric key.

Steps for Proposed plan :

- Providing multifactor authentication.
- Establishing Intrusion Detection System and Prevention System.
- Discovery of Botnets and giving immediate mitigation plan.
- Using encryption and decryption techniques providing optimized solutions.
- Incident Response Plan

11 SECURITY BENEFITS OF CLOUD COMPUTING

Cloud Computing has a lot of potential to improve security for enterprises and the ways it can improve security is described below.

A. Benefits of Scale

It is a fact that all types of security measures which are implemented on a larger scale are cheaper. Hence by adopting Cloud Computing enterprises gets better protection with same amount of money. The security includes all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances, human resources and their management and vetting, hardware and software redundancy, strong authentication, efficient role-based access control and federated identity management solutions by default, which also improves the network effects of collaboration among various partners involved in defense. Along with these benefits, other benefits include:

B. Multiple Locations

The cloud providers by default have economic resources to replicate content and this increases the redundancy and independence from failure. Hence, it provides the disaster recovery.

C. Edge Networks

Cloud Computing provides reliability, quality increase and less local network problems for enterprises by having storage, processing and delivery closer to the network edge.

D. Improved Timelines of Response

Cloud providers have larger to incidents or well-run-larger-scale systems. These systems help in improved timelines of response e.g. because of the early detection of new malware deployments, it can develop more effective and efficient incident response.

12 CONCLUSION

Cloud computing opens several new trends, like using software that are not present on your computer, accessing data from anywhere. One of the big advantages of cloud computing is virtualization, but we can use cloud computing properly only if it provides reliable security. Cloud computing is mostly used because it provides much storage space to its user, so it becomes necessary to provide security to that data. There are many security algorithms, but security of all these algorithms can be broken by anyone. So it is very necessary to make security of cloud more strong. Cloud computing prove a very successful application for organisations. Because organisations have large amount of data to store and cloud provides that space to its user and also allows its user to access their data from anywhere anytime easily. As people are saving their personal and important data to clouds, so it becomes a major issue to store that data safely. Many algorithms exist for the data security like DES, AES, and Triple DES. These are symmetric key algorithms in which a single key is used for encryption and decryption whereas RSA, Diffie-Hellman Key Exchange and Homomorphic equations are asymmetric, in which two different keys are used for encryption and decryption. After reviewing all

the algorithms, the author suggests that no one algorithm is giving better security. Every algorithm has certain advantages and disadvantages so that we have to combine the best features of all algorithms and give the optimized solution.

REFERENCES

[1] Jing-Jang Hwang, Taoyuan, Taiwan,Yi-Chang Hsu, Chien-Hsing Wu, ABusiness Model for Cloud Computing Based on a Separate Encryptionand Decryption Service, in International Conference on InformationScience and Applications (ICISA), pages 1-7, 2011.

[2] Junzuo Lai, Deng R H, Chaowen Guan, JianWeng, Attribute-BasedEncryption With Verifiable Outsourced Decryption, *in IEEE Transactions on Information Forensics and Security, vol. 8(8), pages 1343-1354*,2013.

[3] FatemiMoghaddamF,KarimiO,Alrashdan M T, A Comparative Studyof Applying Real-Time EncryptioninCloud Computing Environments, *inIEEE 2nd International Conference onCloudNetworking (CloudNet),pages 185-189*, 2013.

[4] Brian Hay, Kara Nance, Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" Proceedings of the 44th Hawaii International Conference on System Sciences, pp.1-7, 2011.

[5] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering, Volume I, ISBN: 978-988-19251-3-8; ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online) , 2012.

[6] Kevin Curran, Sean Carlin and Mervyn Adams, "Security issues in cloud computing", Elixir Network Engg.38 (2011), pp.4069-4072, August 2011.

[7] Randeep Kaur, Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (ISSN 2319 - 4847),Volume 3 Issue 3, pp.171-176, March 2014.

[8] Rashmi Nigoti, Manoj Jhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of Emerging Technologies in Computational and Applied Sciences,Vol. 4, pp.141-146, March-May 2013.

[9] Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[10] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ," Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[11] Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[12] F. A. Alvi,, B.S Choudary, N. Jaferry, E.Pathan, "A review on cloud computing security issues & challanges".